JOURNAL OF ALGEBRA **184,** 199–206 (1996)
ARTICLE NO. 0255

A Note on 2-Automorphic 2-Groups

Bettina Wilkens

Fachbereich Mathematik, Institut für Algebra und Geometrie, Martin-Luther-Universität, 06099 Halle (Saale), Germany

Communicated by Gernot Stroth

Let p be a prime, P a finite p-group on whose set of elements of order p $\operatorname{Aut}(P)$ acts transitively; then P must be abelian or a 2-group [Shul], in the latter case called a 2-automorphic 2-group. In 1976, F. Gross [Gro] established the following theorem on 2-automorphic 2-groups:

Let P be a finite 2-group with more than one involution and on whose set of involutions $\operatorname{Aut}(P)$ acts transitively; then $\Omega_1(Z(P))$ contains all the involutions of P, $|P|$ is a power of $2^m := |\Omega_1(Z(P))|$, and one of the following holds:

1. *P is homocyclic*.

2. *P has exponent 4 and nilpotence class 2, $|P| = 2^{2m}$ or 2^{3m}, and $P' = \Phi(P) = Z(P) = \Omega_1(Z(P))$.*

3. *P has exponent 8 and nilpotence class 3, P' is homocyclic of order 2^{2m} and exponent 4, $P' = \Phi(P) = C_P(P')$ and $Z(P) = [P, P'] = \{x^4 \mid x \in P\} = \Omega_1(P)$. Furthermore, $|P| \geq 2^{4m}$.*

Gross conjectured in [Gro] that there were no groups in 3 and that every group in 2 was a Suzuki 2-group, i.e., a nonabelian 2-group P on whose set of involutions a cyclic subgroup of $\operatorname{Aut}(P)$ acts transitively; Suzuki 2-groups were shown to exist by G. Higman [Hig]. In 1981, E. G. Bryukhanova showed in [Bry] that the only groups in 2 of order 2^{3m} are Suzuki 2-groups. The purpose of this paper is to establish the following theorem:

THEOREM. *Every 2-automorphic 2-group is of class at most 2.*

So let G be a finite 2-group of class 3 which has more than one involution; suppose $\operatorname{Aut}(G)$ acts transitively on the set of involutions of G.

0021-8693/96 $18.00

As G' is homocyclic, $\mathrm{Aut}(G)$ acts transitively on the set of maximal subgroups of $Z(G)$ and of G', as well as on the elements of $G'/Z(G) \setminus \{1\}$. Furthermore, we have $Z_2(G) \subseteq C_G(G') \subseteq G'$.

Notation.

$$
\begin{array}{lll}
Z := Z(G), & |Z| = 2^m. & \\
UG'/G' := \overline{U}, & \bar{x} := xG' & \text{for } U \leq G, x \in G. \\
UZ/Z := \tilde{U}, & \tilde{x} := xZ & \text{for } U \leq G, x \in G. \\
\text{For } U \lessdot Z & \text{let } 2^t := |Z(G/U)/(Z/U)|. & \\
2^k := |\overline{G}|. & &
\end{array}
$$

LEMMA 1. *Let* $M \subseteq \tilde{G} \setminus \tilde{G}'$; *suppose* $\mathrm{Aut}(G)$ *acts on* M *and that, if* $\tilde{x} \in M$, *then* $\tilde{x}\tilde{G}' \subseteq M$. *Let* $N := \{\bar{x} \in \overline{G} \mid \tilde{x} \in M\}$. *Then* $2^m - 1 \mid |N|$.

Proof. The order of any $g \in G$ is uniquely determined by $\bar{g}$; for g of order 8, g^4 is uniquely determined by $\tilde{g}$; likewise g^2 is uniquely determined by $\tilde{g}$ for g of order 4. Thus the stabilizer of $\bar{g}$ in $\mathrm{Aut}(G)$ fixes an involution. So our assumptions on M imply $2^m(2^m - 1) \mid |M|$, so $2^m - 1 \mid |N|$.

DEFINITION. For $l \in \mathbb{N}_0$ let $\tilde{M}_l := \{\tilde{x} \in \tilde{G} \setminus \tilde{G}' \mid |C_{G'}(x)/Z| = 2^l\}$. Since $\mathrm{Aut}(G)$ acts on $\tilde{M}_l$, we have $2^m - 1 \mid |M_l|$ with $M_l = \{\bar{x} \mid \tilde{x} \in \tilde{M}_l\}$ by Lemma 1. Let $0 \leq l_1 < \cdots < l_q$ be those natural numbers l for which M_l is nonempty; let $(2^m - 1)a_i = |M_{l_i}|$.

LEMMA 2. *Let* $\tau \in G' \setminus Z$ *and* $U \lessdot Z$. *Then* $|\overline{C_G(\tau)}| = |\overline{C_G(G'/U)}| = 2^{k-m+t}$.

Proof. For $x \in G$ we have $\|[G', x]\| = |G'/C_{G'}(x)|$; so, for $x \in M_{l_i}$, $[G', x]$ is contained in exactly $2^{l_i} - 1 = |\overline{C_{G'}(x)} \setminus \{1\}|$ maximal subgroups of Z. So we have

$$
\begin{aligned}
(2^m - 1)&|\overline{C_G(G'/U)} \setminus \{1\}| \\
&= \left|\left\{(U, \bar{x}) \mid U \lessdot Z, \bar{x} \in \overline{G} \setminus \{1\}_1 [x, G'] \subseteq U\right\}\right| \\
&= (2^m - 1)\left(a_1(2^{l_1} - 1) + \cdots + a_q(2^{l_q} - 1)\right) \\
&= \left|\left\{(\tilde{\sigma}, \bar{x}) \mid \sigma \in G' \setminus Z, \bar{x} \in \overline{G} \setminus \{1\} [x, \sigma] = 1\right\}\right| \\
&= (2^m - 1)|\overline{C_G(\tau)} \setminus \{1\}|.
\end{aligned}
$$

Hence $|\overline{C_G(\tau)}| = |\overline{C_G(G'/U)}|$. Finally, let $U \lessdot Z$, $\tau \in G' \setminus Z$. We have

$$\begin{aligned}(2^m - 1)&|Z(G/U)/(Z/U) \setminus \{1\}| \\ &= (2^m - 1)|\{V \lessdot Z \mid [\tau, G] \subseteq V\}| = (2^m - 1)(2^t - 1),\end{aligned}$$

and therefore $\|[G,\tau]\| = 2^{m-t}$. So $|\overline{C_G(\tau)}| = 2^{k-m+t}$.

LEMMA 3. $|\overline{G}| = 2^{2m}$ *and* $G' \neq \Omega_2(G)$.

Proof. Fix $U \lessdot Z$ and let $C := C_G(G'/U)$. Then $|\overline{C}| = 2^{k-m+t}$, according to Lemma 2. Furthermore, $[C, C, G] \subseteq [C, G, C] \subseteq U$ by the Three-Subgroup Lemma. Thus $|\tilde{C}'| \leq 2^t$.

Now we look at a chain $\tilde{C} = \tilde{C}_0 \trianglerighteq \tilde{C}_1 \cdots \trianglerighteq \tilde{C}_r$ with the following properties: Let C_i be the full preimage of $\tilde{C}_i$ in G; if $[C_i, C_i'] \neq 1$, pick $U_{i+1} \lessdot Z$ such that $[C_i, C_i'] \nsubseteq U_{i+1}$ and let $C_{i+1} = C_{C_i}(C_i'/U_{i+1})$. Then $[C_{i+1}', C_i] \subseteq [C_i, C_{i+1}, C_{i+1}] \subseteq U_{i+1}$ by the Three-Subgroup Lemma, so $\tilde{C}_{i+1}' \neq \tilde{C}_i'$. Thus we must finally arrive at i with $[C_i, C_i'] = 1$; then let $r = i$.

We claim that for $0 \leq l \leq r$ we have

$$|\tilde{C} : \tilde{C}_l| \leq |\tilde{C}' : \tilde{C}_l'| \leq 2^t.$$

The second inequality follows from $|\tilde{C}'| \leq 2^t$. In order to establish the first, we proceed by induction on l. If $l = 0$, there is nothing to prove. Let $l < r$ and assume C_l to obey the inequality asserted. We have $[C_{l+1}, C_l'] \subseteq U_{l+1}$. As G' is homocyclic of exponent 4 and $\Omega_1(G) = Z$, the group $V := \tilde{C}_l'/C_{\tilde{C}_l'}(C_l/U_{l+1})$ is elementary abelian and therefore can be viewed as a GF(2)-vectorspace; then $\tilde{C}_l/\tilde{C}_{l+1}$ embeds into V^* via the mapping $x \mapsto \varphi_x$, where $\varphi_x\colon v \mapsto [w, x]U_{l+1}$ for $x \in C_l$ with $w \in C_l'$ and $v = \tilde{w}C_{\tilde{C}_l'}(C_l/U_{l+1})$. Since $\tilde{C}_{l+1}' \subseteq \tilde{C}_{C_l'}(C_l/U_{l+1})$ we have $|\tilde{C}_l' : \tilde{C}_{l+1}'| \geq |V|$. As $\dim(V) = \dim(V^*)$ the inductive assumption yields

$$|\tilde{C} : \tilde{C}_{l+1}| = |\tilde{C} : \tilde{C}_l|\,|\tilde{C}_l : \tilde{C}_{l+1}| \leq |\tilde{C}' : \tilde{C}_l'|\,|\tilde{C}_l' : \tilde{C}_{l+1}'|.$$

If $|\tilde{C} : \tilde{C}_r| = 2^t$, the proposition yields $C_r' \subseteq Z$.

Next we will establish an upper bound for $|C_r|$. We have $[C_r, C_r'] = 1$. For $x \in G$, $o(x) = 4$ and $g \in G$ we have $1 = [x^2, g] = [x, g]^2[x, g, x]$; i.e., every element of $[x, G]$ is inverted by x. Thus $[\Omega_2(C_r), C_r] \subseteq Z$. In particular $\Omega_2(C_r) \supseteq G'$ is of class ≤ 2 and of exponent 4.

Now let $x, y \in C_r$ both be of order 8 and suppose $\tilde{x}^2 = \tilde{y}^2$. Then $(xy)^2 = x^2y^2[y, x] \in [y, x]Z$. Furthermore,

$$[x, y] = ([x, y])^{x^{-1}} = (y^{-1}xyx^{-1})(x^{-2}x^2) = [y, x].$$

Thus $[y, x] \in Z$ and $o(xy) = o(xy^{-1}) = 4$. So the (well-defined) mapping $x\Omega_2(C_r) \mapsto \tilde{x}^2$, $x \in C_r$, is an injection, which implies $|C_r : \Omega_2(C_r)| \le 2^m$. Now $\Omega_2(C_r)$ meets every requirement imposed upon the group P in [Hup, VIII, 5.4]; since $G' \subseteq \Omega_2(C_r)$, we get $|\Omega_2(C_r) : G'| \le 2^m$.

All in all, we have $k \le m - t + t + 2m = 3m$. Since m is a divisor of k, we need only exclude the case $k = 3m$. So suppose $k = 3m$; then $|C : C_r| = 2^t$, so $C_r' \subseteq Z$. Furthermore, $|C_r : \Omega_2(C_r)| = 2^m$. So $\tilde{G}' \setminus \{1\} = \{\tilde{x}^2 \mid x \in C_r\}$ because the mapping $x\Omega_2(C_r) \mapsto \tilde{x}^2$, $x \in C_r$, is an injection. Since $C_r' \subseteq Z$, this implies $[C_r, G'] = 1$, contradiction.

The only assertion left to be established is $G' \not\supseteq \Omega_2(G)$. Since $k \ge 2m$, the assumption $\Omega_2(C_r) = G'$ again yields the consequences $|C : C_r| = 2^t$ and $|C_r : \Omega_2(C_r)| = 2^m$. This implies again that $\tilde{G}' \setminus \{1\} = \{\tilde{x}^2 \mid x \in C_r\}$ and that $C_r \subseteq C_G(G') = G'$, which enforces $k = m$, contradiction.

DEFINITION. Any $x \in G$ of order 8 and such that no element of $G' \setminus Z$ is inverted by x will be said to have property $(*)$.

LEMMA 4. *There is $x \in G$ with property $(*)$.*

Proof. Let $\tilde{\tau} \in \tilde{G}' \setminus \{1\}$; according to Lemmas 2 and 3, we have $a_1 + \cdots + a_q = 2^m + 1$ and

$$|\overline{C_G(\tau)} \setminus \{1\}| = 2^{m+t} - 1 = a_1(2^{l_1} - 1) + \cdots + a_q(2^{l_q} - 1). \tag{1}$$

Let $x \in G$; the set of elements of G' inverted by x is a subgroup of G' containing Z. According to Lemma 1, the number $|N_n| = |\{\bar{x} \in \overline{G} \setminus \{1\} \mid |\{\tilde{\sigma} \in G' \mid \sigma^x = \sigma^{-1}\}| = 2^n\}|$, where $n \in \mathbb{N}$, is divisible by $2^m - 1$. Let $\tau \in G' \setminus Z$ and $M := \{\bar{x} \in \overline{G} \mid \tau^x = \tau^{-1}\}$. Then $|M| = 2^{m+t}$, because, by Lemma 3, there are elements of G of order 4 outside G', and, since $Z_2(G) \subseteq G'$, we find y of order 4 with $\tilde{\tau} \in [\tilde{G}, \tilde{y}]$. Any such y inverts τ. So $|\overline{N_G(\langle \tau \rangle)}| = 2^{m+t+1}$ by Lemmas 2 and 3. Let $0 \le n_1 < \cdots < n_p$ be those numbers n with $N_n \ne \emptyset$ and let $|N_{n_i}| = (2^m - 1)b_i$. Then $b_1 + \cdots + b_p = 2^m + 1$ and for $\bar{x} \in N_{n_i}$ there are $2^{n_i} - 1$ elements $\tilde{\tau} \in \widetilde{G'} \setminus \{1\}$ with τ inverted by x. Thus

$$\begin{aligned}(2^m - 1)^{-1} \cdot \left|\left\{(\bar{x}, \tilde{\sigma}) \mid \bar{x} \in \overline{G} \setminus \{1\}, \sigma \in G' \setminus Z_1 \sigma^x = \sigma^{-1}\right\}\right| \\ = 2^{m+t} = b_1(2^{n_1} - 1) + \cdots + b_p(2^{n_p} - 1).\end{aligned} \tag{2}$$

As $a_1 + \cdots + a_q = b_1 + \cdots + b_p$, subtraction of (1) from (2) yields

$$2^{n_1}b_1 + \cdots + 2^{n_p}b_p - \left(2^{l_1}a_1 + \cdots + 2^{l_q}a_q\right) = 1,$$

so $l_1 = 0$ or $n_1 = 0$. Suppose $l_1 = 0$; since an element of G of order 8 centralizes its square, there is $x \in G$ of order 4 and such that $C_{G'}(x) = Z$.

Now let D be the full preimage of $C_{\tilde{G}}(\tilde{x})$. Then $\Phi(D) \subseteq Z$, and thus $\mathrm{cl}(D) \leq 2$, $\exp(D) \leq 4$. Now we can again make use of [Hup, VIII, 5.4] to establish $|\overline{D}| \leq 2^m$, so $[\langle \tilde{x} \rangle, \tilde{G}] = \tilde{G}'$. Since for $g \in G$, $h \in G$, $o(h) = 4$ we have $1 = [h^2, g] = [h, g]^2[h, g, h]$ every element of G' is inverted by x. As $C_G(G') = G'$, this yields $E := \langle x \rangle G'$ char G; but then, by Lemma 1, $|\langle \bar{x} \rangle|$ is divisible by $2^m - 1$, so G contains exactly on involution, which contradicts our initial assumptions about G.

Thus we have $n_1 = 0$; since $Z_2(G) = G'$, every $y \in G \setminus G'$ of order 4 inverts some element of G'. The assertion has been established.

LEMMA 5. *Let $x \in G$ have property $(*)$. Then $C_G(x^2)/Z = C_{\tilde{G}}(\tilde{x})$; in particular, whenever $\tilde{y}^2 = \tilde{x}^2$ for $y \in G$, xy is of order* 4.

Proof. Let $h \in C_G(x^2)$. Then $1 = [x^2, h] = [x, h]^2[x, h, x]$. Thus $[x, h]$ is of order at most 2 because x has property $(*)$. Let $\tilde{y}^2 = \tilde{x}^2$; then y centralizes x^2, so $\tilde{y}$ centralizes $\tilde{x}$, as has just been proved. Therefore $(xy)^2 Z = x^2 y^2 [x, y] Z = Z$.

LEMMA 6. *Let E be an extraspecial* 2*-group of order* 2^{2n+1}. *The number of involutions of E is either* $2^{2n} + 2^n - 1$ *or* $2^{2n} - 2^n - 1$, *differing according to isomorphism type*.

Proof. See, e.g., [Tay, 11.5]. One must count the singular vectors of an orthogonal vectorspace over GF(2), multiply by 2, and add 1.

Fix $V \lessdot G'$; then G/V is a product $Z(G/V)E$, where E is extraspecial and $Z(G/V) \cap E = G'/V$; let the order of E be 2^{2n+1}. Let $a := |\{\bar{x} \in \overline{G} \mid o(x) = 8\}|$. With notation thus fixed, we have

LEMMA 7. $a = (2^m - 1)(2^m - 2^{m-n})$ *and $Z(G/V)$ is elementary abelian.*

Proof. Let B be the set of elements of G/V of order 4, $b = |B|$. The elements $x \in G$ of order 8 with $x^2 \notin V$ are exactly those x for which $xV \in B$. Since V has 2^{m-1} (one-dimensional) complements in $\widetilde{G'}$ we have $a = 2^{-1}2^{1-m}(2^m - 1)b$. First, suppose that $Z(G/V)$ contains an element of order 4. Then it has 2^{2m-2n} such elements; since $Z(G/V) \cap E = G'/V$, we have

$$b = 2^{2m-2n-1}(2^{2n} \pm 2^n) + 2^{2m-2n-1}(2^{2n} \mp 2^n) = 2^{2m}.$$

The first term on the left hand side of the equation is the number of products eh, $e \in E$, $h \in Z(G/V)$, $o(e) \leq 2$, $o(h) = 4$; the second term, the number of products eh, e of order 4, $o(h) \leq 2$.

The foregoing yields $a = (2^m - 1)2^m$. Now let c be the number of $\bar{x} \in \overline{G} \setminus \{1\}$, where x is of order 4; by Lemma 3, $c = 2^{2m} - 1 - a$, so our current assumption implies $c = 2^m - 1$. Now let $y \in G$ be an element which has $(*)$; there are $(2^m-1)^{-1}a = 2^m$ elements $\overline{w} \in \overline{G} \setminus \{1\}$ with $\tilde{y}^2 = \tilde{w}^2$. With w so chosen, we have $o(wy) = 4$ by Lemma 5. This lemma also says that $[wy, y] \in Z$. Thus, if $c = 2^m - 1$, each element x of G of order 4 has $[x, y] \in Z$, so centralizes y^2. However, we have shown that $G' \not\supseteq \Omega_2(G)$ char G; since $\mathrm{Aut}(G)$ is transitive on the involutions of $\tilde{G}'$, we get $[\Omega_2(G), G'] = 1$. But $G' = C_G(G')$, contradiction.

Thus $Z(G/V)$ is elementary abelian, so E has an elementary abelian normal complement of order 2^{2m-2n} in G/V. Thus $b = 2^{2m-2n}(2^{2n} \pm 2^n)$ $= 2^{2m} \pm 2^{2m-n}$. Therefore either $m = n$ and $a = 2^{2m} - 1 = \overline{G} \setminus \{1\}$ by Lemma 3, or $a = (2^m - 1)(2^m - 2^{m-n})$, as asserted. But the former cannot occur, because, by Lemma 3, $\overline{\Omega_2(G)} \neq 1$; so $c > 0$.

Proof of Theorem. Fix $\tau \in G' \setminus Z$ and let $D := N_G(\langle \tau \rangle)$. Let $x, y \in G$ be elements having $(*)$ and such that $\tilde{x}^2 = \tilde{y}^2 = \tilde{\tau}$.

1. We have $\tilde{D} = N_{\tilde{G}}(\langle \tilde{x} \rangle) > \widetilde{C_G(\tau)}$.

Proof. Lemma 7 says that for $V \lessdot G'$, $Z(G/V)$ is elementary abelian; for any $g \in G$ of order 8, we thus have $\tilde{g}^2 \in [\langle \tilde{g} \rangle, G]$. Otherwise, one would find some $U \lessdot G'$ with $g^2 \notin U$ but $[g, G] \subseteq U$. Since $\tilde{G}$ is of class 2, this implies the existence of $h \in G$ with $\tilde{x}^{\tilde{h}} = \tilde{x}^{-1}$. According to Lemma 5, we have $C_G(x^2)/Z = C_{G/Z}(\tilde{x})$, so, as τ is likewise inverted by h, the assertion is established.

2. $\tilde{x}\tilde{y} \in Z(\tilde{D})$.

Proof. Any $\tilde{d} \in \tilde{D}$ either centralizes or inverts both $\tilde{x}$ and $\tilde{y}$; so $(\tilde{x}\tilde{y})^{\tilde{d}} = \tilde{x}^{-1}\tilde{y}^{-1} = \tilde{x}\tilde{y}\tilde{x}^4 = \tilde{x}\tilde{y}$ for $d \in D$.

3. $Z(\tilde{D}) \setminus \tilde{G}' = \{\tilde{g} \in \tilde{G} \setminus \tilde{G}' \mid (xg)^2 \in x^2 Z, (xg)$ has property $(*)\}$.

Proof. We have to show that for $\tilde{u} \in Z(\tilde{D})$, (xu) has $(*)$. Assume the contrary. Then one finds $\sigma \in G' \setminus Z$ with $\sigma^{xu} = \sigma^{-1}$. There is $z \in G$ having $(*)$ and such that $\tilde{z}^2 = \tilde{\sigma}$. Now $\tilde{x}\tilde{u}$ inverts $\tilde{z}$, so z centralizes $(xu)^2$. According to 1, $D > C_G(\tau)$, so u is of order 4 and $(xu)^2 \in \tau Z$. But then $z \in D$ so $\tilde{z}$ centralizes both $\tilde{x}$, by 1, and $\tilde{u}$, by choice of u, contradiction.

Let Γ be the graph with vertex set $\{\bar{g} \in \overline{G} \mid o(g) = 4, \tilde{\tau} \in [\tilde{G}, \tilde{g}]\}$. This set is nonempty because of Lemma 3 and because $C_G(G') = G'$. In view of 1, its elements are exactly those $\bar{g}$ with g of order 4 and $g \in D \setminus C_G(\tau)$. Two vertices $\bar{g}$, $\overline{h}$ of Γ are to be joined by an edge if and only if $(gh)^2 \in \tau Z$ and (gh) has $(*)$. Let $B = \{\bar{x} \mid \tilde{x}^2 = \tilde{\tau}, x$ has $(*)\}$ and $b = |B|$. Let $\bar{g}$ be a vertex of Γ and $x \in G$ such that $\bar{x} \in B$. So $\tilde{x}$ is inverted by $\tilde{g}$ according to 1, so $\widetilde{gx}^2 = \tilde{g}^2\tilde{x}^2[\tilde{x}, \tilde{g}] = \tilde{1}$. Thus Γ is b-regular. If $\bar{g}$, $\overline{h}$ and, respectively, $\overline{h}$, $\overline{k}$ are adjacent vertices of Γ, then $(gk) \in (ghhk)Z$. So gk is of order 4 by Lemma 5, so Γ contains no triangles.

Next we will describe the connected components of Γ. To this end, let $P := (\bar{g}_1, \dots \bar{g}_r)$ be a path in Γ with $\bar{g}_i \neq \bar{g}_j$ if $i \neq j$, $1 \leq i \leq j \leq r$. Furthermore, all neighbours of $\bar{g}_1$ as well as those of $\bar{g}_n$ are to be among the vertices of P. For i, $i + 2 \leq r$, we have $\bar{g}_i \bar{g}_{i+2} = \bar{g}_i \bar{g}_{i+1} \bar{g}_{i+1} \bar{g}_{i+2}$, i.e., $\tilde{g}_i \tilde{g}_{i+2} \in Z(\tilde{D})$ by 2.

Therefore, we can prove inductively that $\tilde{g}_1 \tilde{g}_{2k-1} \in Z(\tilde{D})$ for $2k - 1 \leq r$; from this we get, using 3, that $\bar{g}_1$ is adjacent to $\bar{g}_{2k}$ as long as $2k \leq r$, because $\tilde{g}_1 \tilde{g}_{2k} = \tilde{g}_1 \tilde{g}_{2k-1} \tilde{g}_{2k-1} \tilde{g}_{2k}$. Since Γ has no triangles, $r \geq 2b$. As $\bar{g}_1$ and $\bar{g}_{2b}$ are adjacent, the vertices $\bar{g}_1, \dots, \bar{g}_{2b}$ form a circle. Therefore, we can permute the numbers $1, \dots, 2b$ cyclically and let every $a \leq 2b$ take the role of $\bar{g}_1$ in the just completed argumentation. Thus

$$\text{If } a, c \leq 2b, a \equiv c \pmod 2, \text{ then } \tilde{g}_a \tilde{g}_c \in Z(\tilde{D}).$$

$$\text{If } a, c \leq 2b, a \not\equiv c \pmod 2, \text{ then } \bar{g}_a \text{ is adjacent to } \bar{g}_b.$$

So we have: Each of $\bar{g}_1, \dots, \bar{g}_{2b}$ has all of its b neighbours among $\bar{g}_1, \dots, \bar{g}_{2b}$. So $r = 2b$ and the vertices of P are exactly those of a connected component of Γ. Furthermore, every such component is a complete bipartite graph $K(b, b)$. The number of edges of Γ therefore equals eb^2, where e is the number of connected components. Thus

$$\left|\left\{\left(\bar{g}, \bar{h}\right) \mid o(g) = o(h) = 4, \left(\bar{g}, \bar{h}\right) \text{ is an edge of } \Gamma\right\}\right| = 2eb^2.$$

On the other hand, we have: Let $0 \leq r_1 < \cdots < r_q$ be all of the numbers r for which there is $x \in G \setminus G'$ of order 4 with $\|[\tilde{G}, \langle \tilde{x} \rangle]\| = 2^r$. The number $c'_r := |\{\bar{x} \in \overline{G} \setminus \{1\} \mid o(x) = 4, \|[\tilde{G}, \langle \tilde{x} \rangle]\| = 2^r\}|$ is divisible by $2^m - 1$ for any r by Lemma 1. Let $c'_{r_i} = (2^m - 1)c_i$. Thus $c_1 + \cdots + c_q = 2^{m-n} + 1$ by Lemmas 3 and 7. Furthermore, by the definition of the numbers r_i, we have $(2^m - 1)|\{\bar{x} \in \overline{G} \setminus \{1\} \mid o(x) = 4, \tilde{\tau} \in [\tilde{G}, \tilde{x}]\}| = (2^m - 1)(c_1(2^{r_1} - 1) + \cdots + c_q(2^{r_q} - 1))$. So the number of vertices of Γ is $c_1(2^{r_1} - 1) + \cdots + c_q(2^{r_q} - 1)$. As Γ is b-regular, this yields

$$\begin{aligned} \left|\left\{\left(\bar{g}, \bar{h}\right) \mid \left(\bar{g}, \bar{h}\right) \text{ is an edge of } \Gamma\right\}\right| &= \left((2^{r_1} - 1)c_1 + \cdots (2^{r_q} - 1)c_q\right)b \\ &= \left(c_1 2^{r_1} + \cdots c_q 2^{r_q} - \left(2^{m-n} + 1\right)\right)b \\ &= 2b^2 e. \end{aligned}$$

Thus $(2^{r_1}c_1 + \cdots + 2^{r_q}c_q) = 2be + 2^{m-n} + 1$. So either $r_1 = 0$ or $m = n$. In the first case, $Z_2(G) > G'$, a contradiction. In the second case, we have $\tilde{G}' = [\tilde{G}, \langle \tilde{x} \rangle]$ for every $x \in G \setminus G'$. In particular, we can choose x of order 4 by Lemma 3; but then x inverts every element of G'. Then $E := \langle x \rangle G'$ char G, because $C_G(G') = G'$; but then, by Lemma 1, G contains exactly one involution, contradiction.

REFERENCES

[Bry] E. G. Bryukhanova, Automorphism groups of 2-automorphic 2-groups, *Algebra Logic* **20** (1981), 1–12.

[Gro] F. Gross, 2-Automorphic 2-groups, *J. Algebra* **40** (1976), 348–353.

[Hig] G. Higman, Suzuki 2-groups, *Illinois J. Math.* **7** (1963), 79–96.

[Hup] B. Huppert and N. Blackburn, ''Finite groups II,'' Springer-Verlag, Berlin/New York, 1982.

[Shul] E. Shult, On finite automorphic algebras, *Illinois J. Math.* **13** (1969), 625–653.

[Tay] D. E. Taylor, ''The Geometry of the Classical Groups,'' Heldermann, Berlin, 1992.